Scottish Cyber Coordination Centre

Daily threat bulletin

24 July 2024

Vulnerabilities

Microsoft Defender Flaw Exploited to Deliver ACR, Lumma, and Meduza Stealers

The Hacker News - 24 July 2024 12:45

A now-patched security flaw in the Microsoft Defender SmartScreen has been exploited as part of a new campaign designed to deliver information stealers such as ACR Stealer, Lumma, and Meduza.Fortinet FortiGuard Labs said it detected the stealer campaign targeting Spain, Thailand, and the U.S. using booby-trapped files that exploit CVE-2024-21412 (CVSS score: 8.1).

CISA Adds Twilio Authy and IE Flaws to Exploited Vulnerabilities List

The Hacker News - 24 July 2024 12:26

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added two security flaws to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation. The vulnerabilities are listed below - CVE-2012-4792 (CVSS score: 9.3) - Microsoft Internet Explorer Use-After-Free Vulnerability - CVE-2024-39891 (CVSS score: 5.3) - Twilio Authy Information Disclosure vulnerability.

Threat actors and malware

Chinese hackers deploy new Macma macOS backdoor version

BleepingComputer - 23 July 2024 20:33

The Chinese hacking group tracked as ‘Evasive Panda’ was spotted using new versions of the Macma backdoor and the Nightdoor Windows malware.

Hackers abused swap files in e-skimming attacks on Magento sites

Security Affairs - 23 July 2024 18:28

Threat actors abused swap files in compromised Magento websites to hide credit card skimmer and harvest payment information. Security researchers from Sucuri observed threat actors using swap files in compromised Magento websites to conceal a persistent software skimmer and harvest payment information.

Chinese Espionage Group Upgrades Malware Arsenal to Target All Major OS

Infosecurity Magazine - 23 July 2024 16:00

Symantec said Chinese espionage group Daggerfly has updated its malware toolkit as it looks to target Windows, Linux, macOS and Android operating systems.

BreachForums v1 hacking forum data leak exposes members’ info

Scottish Cyber Coordination Centre

BleepingComputer - 23 July 2024 16:24

The private member information of the BreachForums v1 hacking forum from 2022 has been leaked online, allowing threat actors and researchers to gain insight into its users.

New ICS Malware 'FrostyGoop' Targeting Critical Infrastructure

The Hacker News - 23 July 2024 17:24

Cybersecurity researchers have discovered what they say is the ninth Industrial Control Systems (ICS)-focused malware that has been used in a disruptive cyber attack targeting an energy company in the Ukrainian city of Lviv earlier this January.Industrial cybersecurity firm Dragos has dubbed the malware FrostyGoop.

UK related

Prolific DDoS Marketplace Shut Down by UK Law Enforcement

Infosecurity Magazine - 23 July 2024 09:30

The UK's National Crime Agency has infiltrated the DigitalStress marketplace, which offers DDoS capabilities.